FIREWALL CONFIGURATION AND TESTING USING UFW ON KALI LINUX

Objective:

To configure and test basic firewall rules using UFW (Uncomplicated Firewall) on Kali Linux.
The goal was to block and allow specific network traffic, verify functionality, and document the steps.

Tools Used:

- Kali Linux
- UFW (Uncomplicated Firewall)
- Telnet (for testing blocked ports)
- Terminal

Steps Performed:

1. Installed and Enabled UFW

- Updated package list:
```
sudo apt update
```
- Installed UFW:
```
sudo apt install ufw -y
```
- Enabled UFW:
```
sudo ufw enable
```

Purpose:
This ensured that the firewall service was running and ready to manage traffic filtering.

2. Verified Firewall Status
```
sudo ufw status verbose
```

Output:
Showed the firewall was active and listed the default policies (deny incoming, allow outgoing).

3. Blocked Inbound Traffic on Port 23 (Telnet)
```
sudo ufw deny 23/tcp
```

Purpose:
Blocked insecure Telnet connections which operate on port 23.
This prevents unauthorized remote access attempts using an unencrypted protocol.

Verified using:
```
sudo ufw status numbered
```

4. Tested the Deny Rule

```
telnet localhost 23
```

Result:
The connection was refused or failed, confirming that the Telnet port was successfully blocked.

5. Allowed SSH Traffic on Port 22

```
sudo ufw allow 22/tcp
```

Purpose:
To ensure secure remote management via SSH.
SSH (port 22) provides encrypted access to the system.

Verified using:

```
sudo ufw status numbered
```

Output showed both:

```
22/tcp ALLOW
 23/tcp DENY
```

6. Removed the Telnet Block Rule

```
sudo ufw delete deny 23/tcp
```

or

```
sudo ufw delete [rule_number]
```

Purpose:
To restore the system to its original state after testing.

Verified using:

```
sudo ufw status numbered
```

Output showed Telnet rule removed.

7. Exported Firewall Configuration

```
sudo ufw status verbose > ufw-status.txt
```

Purpose:
Saved the current firewall configuration and rule list for documentation.

8. Disabled UFW (Optional Cleanup)

```
sudo ufw disable
```

Purpose:
To stop the firewall service after completing the test, leaving the system in its default state.

Screenshots Taken:

1. Update Repositories
2. UFW installation
3. UFW initial status (before adding rules)
2. Telnet block rule added (deny 23/tcp)
3. Failed Telnet connection test
4. SSH allow rule added (allow 22/tcp)
5. Telnet rule removed (restored state)
6. Disable UFW

Understanding How Firewall Filters Traffic:

A firewall acts as a barrier between your system and external networks.
It monitors and filters incoming and outgoing packets based on predefined rules.

- Inbound traffic: Data packets coming into your system (e.g., SSH, HTTP requests)
- Outbound traffic: Data packets leaving your system (e.g., browsing)

By using rules:
Allow (permit) → lets traffic through specific ports or services
Deny (block)→ prevents access to insecure or unwanted ports

In this task:

- Port 23 (Telnet) was blocked due to its insecure nature.
- Port 22 (SSH) was allowed to ensure secure remote administration.

Outcome:

Successfully learned how to:

- Install, enable, and manage UFW on Linux
- Add, verify, and remove firewall rules
- Test blocked and allowed ports
- Understand how firewalls filter network traffic

This demonstrates the ability to control access to a Linux system through basic firewall configurations.